North Dakota
Homeland Security
Anti-Terrorism Summary

The North Dakota Open Source Anti-Terrorism Summary is a product of the North Dakota State and Local Intelligence Center (NDSLIC). It provides open source news articles and information on terrorism, crime, and potential destructive or damaging acts of nature or unintentional acts. Articles are placed in the Anti-Terrorism Summary to provide situational awareness for local law enforcement, first responders, government officials, and private/public infrastructure owners.

NDSLIC Disclaimer

Quick Links

North Dakota

Regional

National

International

Banking and Finance Industry

Chemical and Hazardous Materials Sector

Commercial Facilities

Communications Sector

Critical Manufacturing

Defense Industrial Base Sector

Emergency Services

Energy

Food and Agriculture

Government Sector (including Schools and Universities)

Information Technology and Telecommunications

National Monuments and Icons

Postal and Shipping

Public Health

Transportation

Water and Dams

North Dakota Homeland Security Contacts

North Dakota

Army Corps of Engineers drawing down reservoirs. The U.S. Army Corps of Engineers is drawing down 4 of its reservoirs in the Red River watershed to prepare for the flood battle ahead. There is normally no drawdown for Mud Lake, which is downstream of Lake Traverse, near Wheaton, Minnesota, a city located where Minnesota, North Dakota and South Dakota meet. But the Corps is lowering by 2 feet so it can hold more snowmelt. Lake Traverse is already down 2 feet from its usual level, and the Corps plans to lower it another foot by the end of the month. The Corps will begin its final drawdown at Homme Reservoir, near Park River, North Dakota, following a partial drawdown last November. Orwell Reservoir, near Fergus Falls, is targeted to reach its maximum drawdown by March 18. It is currently 9 feet below its usual level with 5 feet remaining. Source: http://www.kttc.com/Global/story.asp?S=14215087

Oil well continues to burn in McKenzie County. The oil well fire in McKenzie County, North Dakota continued to burn for the fourth day, March 10, and it could keeping burning for several more days. The Jaynes well caught fire March 7 in Arnegard. SM Energy, along with Sanjel and Boots and Coots are working in unison to put out the fire. Currently, they have been cleaning away metal and debris from the scene. No one has been killed or injured, but SM Energy is requesting that the McKenzie County ambulance be on standby while they work. "I think the intent is to get in there close, dig a trench, and then using their equipment, cut off the well head and that way they would be able to control the flame," said a spokesman for McKenzie County Emergency Services (MCES). MCES has also been working with the U.S. Environmental Protection Agency and the state health department. The environmental chief said there is no immediate threat. Source: http://www.kfyrtv.com/News_Stories.asp?news=47217

Sheriff: Fire, explosion in ND oil field under investigation. The Burke County, North Dakota sheriff's office said an investigation continued March 7 into the cause of a fire and explosion in the oil field south of Bowbells, North Dakota. A sheriff said in a prepared release that several oil tanks at a salt water disposal site caught fire March 3 and three exploded. He said the fire was contained on site and was allowed by the Powers Lake and Bowbells fire departments to burn itself out. No injuries were reported. Source: http://www.therepublic.com/view/story/14390c5ce22c42389d6794d126117645/ND--Tank-Fire/

Regional

(Minnesota) **12 indicted in Minn. in alleged $10M bank fraud ring.** Twelve people have been charged in a $10 million bank fraud conspiracy that authorities said depended on identity theft by employees in some of America's largest banks, according to a federal indictment unsealed March 9. The indictment accused the defendants of buying and selling identifications and using them to create phony bank and credit card accounts, apply for loans, and get cash. Authorities said the network operated in many states, and bank employees in Minnesota and elsewhere were recruited to obtain

customer information and conduct phony transactions. One defendant, the manager of a Wells Fargo branch, had bank account information for several people in her car and at her home when she was arrested March 9, authorities said. "There's a severe risk to the community regarding the buying and selling of people's personal information," an assistant U.S. attorney said. Source: http://www.foxnews.com/us/2011/03/09/12-indicted-minn-alleged-10m-bank-fraud-ring/

(Minnesota) **Arson suspected.** Officials suspect a fire that destroyed a vacant building on Main Street in South Haven, Minnesota March 5 and threatened the post office two doors down was deliberately set. Firefighters from South Haven and three neighboring towns were able to protect the post office and another vacant building between it. Postal officials closed the building temporarily the week of March 7 because of the strong smell of smoke and moved operations to the Annandale post office. No one was injured in the fire, which started just before 5 p.m. March 5 in a building on the northeast corner of Main and Grant Streets and burned it to the ground. Source: http://www.annandaleadvocate.com/main.asp?FromHome=1&TypeID=1&ArticleID=11035&SectionID=1&SubSectionID=1

(Minnesota) **Employees back to work after bomb threat.** The Lund-Crestline factory in New York Mills, Minnesota, was evacuated March 8 after a bomb threat was reported. At 1:27 p.m., a 911 call was placed and a male caller said, "There is a bomb in the factory," and hung up, according to the New York Mills police chief. Police were in the process of tracking the call. Brunswick Corporation, which owns and operates the factory, evacuated all employees shortly after the call, according to the police chief, who also said streets were blocked off and school buses were rerouted. A team with a bomb-sniffing dog was in the process of checking the entire facility at 4 p.m. The police chief said it would take several hours to check the facility, but once completed and if nothing is found, employees could return to work. The New York Mills Police Department, state patrol, Otter Tail County Sheriff's Office, and New York Mills Fire and Rescue assisted at the scene. Source: http://www.duluthnewstribune.com/event/article/id/17547/publisher_ID/17/

(Minnesota) **Grain bin explodes.** One man sustained minor injuries when a grain bin exploded March 4 in Lansing, Minnesota. Austin Fire Department and Mower County sheriff's deputies responded to a call at around 5:20 p.m. that a small explosion had taken place at the bin, located off County Road 2. The explosion started in the loading area garage, where it blew out a wall, and traveled 60 feet up the grain leg, causing two additional blowouts. Austin's fire chief said the explosions did not cause visible flames, and the grain bin itself was not affected. One employee sustained minor injuries from the explosion and was transported to the Austin Medical Center for precautionary reasons. The cause of the fire is not known, but is likely related to a common dust build-up. No grain was lost as a result of the explosion. Source: http://www.albertleatribune.com/2011/03/07/grain-bin-explodes/

NATIONAL

Poll shows 30 percent of young drivers text at the wheel. A new poll shows young drivers are more likely to use cell phones while driving, and that 30 percent of them have recently texted from behind the wheel, transportation officials said March 7. The release of the poll came as the Department of Transportation (DOT) Secretary called distracted driving "a deadly epidemic." The poll comes from the magazine Consumer Reports, which is working with DOT on creating awareness about the dangers of cell phone use while driving. Among the findings are that 63 percent of respondents under

30-years-old reported using a handheld phone while driving in the past 30 days, DOT said. Thirty percent of the drivers texted from behind the wheel in the same time period according to the survey, which had 1,026 respondents. Older drivers were less likely to talk on the phone behind the wheel, and only 9 percent of those over 30-years-old reported they had recently texted while driving. Source: http://www.reuters.com/article/2011/03/08/us-phones-driving-idUSTRE7270D420110308

INTERNATIONAL

Man held in Scotland over Sweden terror attack. Police in Scotland arrested a 30-year-old man March 8 on suspicion of aiding a suicide bomber who targeted Christmas shoppers in Stockholm, Sweden in December. Strathclyde Police said the suspect, who is not British, was detained just after 6 a.m. in Glasgow as part of an "intelligence-led" operation into the Swedish attack. The Stockholm attacker, an Iraqi-born Swede who went to university in Britain, killed himself and injured two others when explosives he was wearing exploded in a busy shopping street. Police said the suspect arrested March 8 posed no direct threat to Scotland. Sweden's security police said the arrest was the result of joint work between officials in Scotland and Sweden. It said "the investigation, so far, shows that there could be a link between the arrested person and the terrorism act in Stockholm on December 11." Officials have said they suspected the attacker had accomplices. Source: http://news.yahoo.com/s/ap/20110308/ap_on_re_eu/eu_britain_sweden_terrorism

French gov't gives more details of hack: 150 PCs compromised. The French National IT Systems Security Agency released further details of the recent attack on French government computers, saying cyberspies were targeting the Group of Twenty Finance Ministers and Central Bank Governors (G-20) meeting. Around 150 IT staff spent the weekend of March 5 and 6 on a massive cleanup operation to undo the effects of the attack on computers at the French Ministry of Economy, Finances, and Industry, the security agency's director-general said March 7. The attack compromised around 150 of the ministry's 170,000 PCs, the agency director-general said. The attack began with a wave of e-mail messages with malware-laden attachments that exploited then-unknown or unprotected flaws in the software running on the PCs. The attackers had access to mailboxes and servers over the course of several weeks. It took the agency until the week of February 28 to figure out what the Trojan was doing, and just how far it had spread. While attacks on other French government computers were made during this time, none of them appeared to have succeeded, the director-general said. The French budget minister said this latest attack was probably from outside France. Source: http://www.computerworld.com/s/article/9213741/French_gov_t_gives_more_details_of_hack_150_PCs_compromised

Wastewater treatment efficiency may be reduced during severe flu pandemic, research indicates. New research published in the journal Environmental Health Perspectives indicated existing plans for antiviral and antibiotic use during a severe influenza pandemic could reduce wastewater treatment efficiency prior to discharge into receiving rivers, resulting in water quality deterioration at drinking water abstraction points, according to a press release. The research team coupled a global spatially-structured epidemic model that simulates the quantities of antiviral and antibiotics used during an influenza pandemic of varying severity, with a water quality model applied to the Thames catchment in England to predict environmental concentrations. An additional model was then used to assess ecotoxicologic effects of antibiotics and antiviral in wastewater treatment plants (WWTP) and rivers,

the release stated. The team concluded that in a moderate and severe pandemic, nearly all WWTPs (80-100 percent) were projected to exceed the threshold for microbial growth inhibition, potentially reducing the capacity of the plant to treat wastewater. "Our results suggest that existing plans for drug use during an influenza pandemic could result in discharge of inefficiently treated wastewater into the UK's rivers," said the lead author. "The potential widespread release of antivirals and antibiotics into the environment may hasten the development of resistant pathogens with implications for human health during and potentially well after the formal end of the pandemic." Source: http://www.watertechonline.com/municipal-industrial/article/wastewater-treatment-efficiency-may-be-reduced-during-severe-flu-pandemic-research-indicates

Banking and Finance Industry

Nothing Significant to Report

Chemical and Hazardous Materials Sector

NRC says 89 of 104 US nuclear power plants got top marks in 2010. The U.S. Nuclear Regulatory Commission (NRC) has issued its annual assessment letters for nuclear power plant licensees, the agency said March 8. Some 89 of the 104 operating nuclear units in the United States "performed at the highest level" in 2010 and received normal, or baseline, inspections, the agency said. In the 5-column action matrix of NRC's reactor oversight process, Column 1 plants require the least amount of agency oversight, while plants in Column 4 receive the most NRC attention short of a mandated shutdown under "unacceptable performance" criteria of Column 5. Nine power reactors were in Column 2, "needing to resolve one or two items of low safety significance," the agency said. Those units were Brunswick-1 and -2; Calvert Cliffs-2; Farley-1; Ginna; North Anna-2; Susquehanna-1; and Turkey Point-3 and -4. Six units were in Column 3 "with one degraded safety cornerstone," requiring "more NRC inspections, senior management attention and oversight focused on the cause of the degraded performance," the agency said. These units were Oconee-1, -2 and -3; Fort Calhoun; Robinson-2; and Wolf Creek. No reactors were in Column 4 or 5. Source: http://www.platts.com/RSSFeedDetailedNews/RSSFeed/ElectricPower/8634731

(Virginia; Texas) **Two U.S. nuclear power projects delayed.** The U.S. Nuclear Regulatory Commission (NRC) has told Dominion and Luminant in separate letters their license applications to build new nuclear power plants in Virginia and Texas will be delayed by at least 18 months after changes in the design of Mitsubishi Heavy Industries' (MHI) Advanced Pressurized Water Reactor (APWR). Luminant plans to use the 1,700 MWe APWR design for units 3 and 4 at the Comanche Peak nuclear power plant in Texas. Dominion plans to use the APWR for the proposed third unit at the North Anna plant in Virginia. Under the NRC's new schedule for reviewing Luminant's application, the safety review for Comanche Peak units 3 and 4 will be completed by June 2013. The safety review for North Anna unit 3 is now expected to be completed in July 2013. MHI made structural changes to the US-APWR design since the 2008 approval that required performing a new seismic analysis. The NRC is reviewing the new seismic re-analysis technical reports submitted by MHI. Source: http://www.powergenworldwide.com/index/display/articledisplay/0900626969/articles/powergenworldwide/nuclear/reactors/2011/03/US-projects-delayed.html

Groups seek to block transport of nuclear generators. Canadian environmental groups have gone to court to block the shipment of 16 nuclear-plant generators through the St. Lawrence Seaway that runs from the Atlantic Ocean to the Great Lakes in the United States and Canada. A motion to halt the shipment was filed in federal court the week of February 28, and a copy was obtained by the Canadian Press. The Sierra Club and the Canadian Environmental Law Association are asking the court to overturn a decision from the Canadian Nuclear Safety Commission. They have also asked for an injunction to keep the Canadian transport minister from signing off on any other permit or authorization allowing Bruce Power to proceed with the project. Bruce Power wants to ship the 16 steam generators, each the size of a school bus, from an Ontario, Canada, nuclear plant to Sweden, passing through the Great Lakes and cities such as Montreal, Canada along the St. Lawrence. The move is strongly opposed by the Bloc Quebecois, the New Democratic Party, and a number of community organizations. The Canadian Nuclear Safety Commission said thousands of shipments of radioactive medical isotopes and other substances routinely go through that route every year. Source: http://www.ctv.ca/CTVNews/Canada/20110308/nuclear-generators-110308/

(Ohio) **Walkie talkie disrupts safety system at Davis-Besse nuclear plant.** The Davis-Besse nuclear power plant in Oak Harbor, Ohio went "radio-inactive" March 3 — losing its emergency water cooling system for 2 minutes — due to a technician's walkie talkie. The technician used his walkie talkie in a room containing a back-up or auxiliary control panel for a system designed to automatically pump water into the reactor in the event of a catastrophic accident. The radio wave disrupted the signal from the control panel to special pumps and emergency valves that even on stand-by are electrically alive for an instantaneous reaction. In two bursts of conversation lasting 8 seconds and 19 seconds during a 2-minute period, the technician rendered the plant's entire emergency shutdown system inoperable, the company told federal regulators March 3. The company posted a sign on the door to the room warning all employees not to key radios near the sensitive control panel, a company spokesman said. The incident should have never happened, said a nuclear safety engineer with the Union of Concerned Scientists. He said such incidents occurred many times in the early 1980s, so much that the Nuclear Regulatory Commission (NRC) issued a warning bulletin in December 1983. "This hasn't happened in decades," he said. "We will definitely be looking into this," said a spokeswoman for the NRC's regional office in Chicago. Source: http://www.cleveland.com/business/index.ssf/2011/03/davis-besse_nuclear_power_plan_1.html

Commercial Facilities

(Washington) **U.S. arrests man in Martin Luther King Day bomb plot.** A Colville, Washington, man was arrested and charged with attempting to place a bomb along the parade route of a Martin Luther King Jr. holiday celebration in Spokane January 17, the U.S. Justice Department said March 10. The 36-year-old man was charged with one count of attempting to use a weapon of mass destruction, which carries a maximum penalty of life in prison. The other count charges him with illegally possessing an explosive device, which carries up to 10 years in prison. He appeared in federal court in Spokane March 9, and is being held in the Spokane County Jail until an arraignment, tentatively scheduled for March 23, authorities told Reuters. A grand jury is set to meet to consider the charges March 22. A federal law enforcement official said authorities were investigating whether the suspect had ties to white supremacists. Officials from the Southern Poverty Law Center, an Alabama-based civil rights group, said the suspect had been a member of the neo-Nazi National Alliance in 2004. A

spokesman for Joint Base Lewis-McChord, the U.S. Army/Air Force base in Washington state, confirmed he served at the former Fort Lewis Army base from 1996 to 1999 as a fire support specialist. The MLK day parade, attended by about 1,500 people, was quickly rerouted while the city's bomb disposal unit was summoned and safely "neutralized the device," the FBI said at the time. Chemical analysis of the homemade bomb remains "ongoing," the FBI supervisory resident agent told Reuters, declining to confirm reports the bomb contained a white powder antico agulant chemical similar to rat poison. Source: http://www.reuters.com/article/2011/03/10/us-usa-crime-parade-idUSTRE7287A020110310?feedType=RSS&feedName=domesticNews

Communications Sector

(Ohio) **FCC to look at city's satellite dish ban.** The city of Mount Vernon, Ohio's recent announcement it would begin enforcing a ban on satellite dish antennae in front yards of properties within the city might get a close look from the Federal Communications Commission (FCC), Mount Vernon News reported March 9. City ordinance Chapter 1177 regulates the location and construction of dish-type satellite signal receiving antennae within the city. The stated purpose of the regulation is to protect the public health, safety, and welfare of residents. It points specifically to the maintenance of utility easements, fire safety access, prevention of accumulation of noxious weeds and debris, and the reasonable aesthetic concerns of neighborhood property owners. The FCC has rules in place governing what a local governmental group can and cannot do as far as regulating the installation of these types of dish antennae. The FCC Web site on the subject states the commission was directed by Congress in section 207 of the Telecommunications Act of 1996 to regulate installations of video-receiving antennae. The commission enforces the law through its Over-the-Air Reception Devices rule that has been in effect since October 1996. Source: http://www.mountvernonnews.com/local/11/03/09/fcc-to-look-at-citys-satellite-dish-ban

(Wisconsin) **Wisconsin introduces law to ban fake caller IDs.** Republican legislators in Wisconsin have introduced a bill that would make it illegal to use caller ID services that can generate fake numbers, Homeland Security News Wire reported March 8. The law drafted by a Wisconsin senator and a state representative prohibit people from using a fake caller ID number to "defraud, cause harm, or gain anything of value." In 2010, Congress passed a similar bill that banned the use of "phone spoofing" technologies. Companies like Spooftel and Spoofcard allow an individual to choose what number they wish to appear on another person's caller ID when they call. The new bill would allow law enforcement officials to target individuals making prank calls in addition to prosecuting companies that provide spoofing technology. Source: http://homelandsecuritynewswire.com/wisconsin-introduces-law-ban-fake-caller-ids

IPv6 intro creates spam-filtering nightmare. The migration towards IPv6 will make it harder to filter spam messages, service providers warn. While the expansion to IPv6 allows far more devices to have a unique Internet address, it creates many problems for security service providers, who have long used databases of known bad IP addresses to maintain blacklists of junk mail sources. Spam-filtering technology typically uses blacklists as one key component in a multi-stage junk mail filtering process that also involves examining message contents. "The primary method for stopping the majority of spam used by e-mail providers is to track bad IP addresses sending e-mail and block them – a process known as IP blacklisting," explained a senior solutions architect at spam-filtering company Cloudmark.

"With IPv6, this technique will no longer be possible and could mean that e-mail systems would quickly become overloaded if new approaches are not developed." Other technologies also track IP addresses for various purposes, including filtering out sources of denial of service attacks, click fraud, and search engine manipulation. Source: http://www.theregister.co.uk/2011/03/08/ipv6_spam_filtering_headache/

After attacks, Google vows to fortify Android store. Google will build new safeguards into Android Market, its application store for the Android mobile OS, following an attack the week of February 28 that infected thousands of phones and forced the company to wipe the malware remotely from phones, it said March 6. More than 50 applications in the Android Market were found to contain a program called DroidDream, which is capable of stealing information about a mobile device and downloading other malicious applications to the phone. Google addressed the issue March 5, when it confirmed it decided to use a command that remotely erases malicious applications. Android users who have downloaded a malicious application will get an e-mail within 3 days from the address android-market-support@google.com explaining the situation, wrote Android's security lead. In addition to wiping malware, Google is also forcing an update on users called "Android Market Security Tool March 2011" which fixes the security issues DroidDream exploits. Some users may get a notification on their device that a malicious application has been removed Android's security lead wrote. About a day after the vulnerabilities have been fixed, users will receive a second e-mail. Phones running Android versions below 2.2.2 are vulnerable. The issues are fixed in the latest 2.3 version of Android, known as "Gingerbread." Source: http://www.computerworld.com/s/article/9213563/After_attacks_Google_vows_to_fortify_Android_store

CRITICAL MANUFACTURING

American Suzuki Motor Corp. recalls KingQuad ATVs due to fire hazard. Suzuki Manufacturing of America Corporation has issued a recall March 10 for about 29,000 Suzuki KingQuad ATVs. The ATVs were distributed by American Suzuki Motor Corp., of Brea, California; Montgomery Motors Ltd., of Honolulu, Hawaii; and Suzuki del Caribe Inc., of Rio Piedras, Puerto Rico. Some KingQuad ATV's plastic fuel tanks were improperly manufactured and can develop a fuel leak, posing a fire hazard. American Suzuki has received 19 reports of fuel leaking from the recalled ATVs. No injuries have been reported. The vehicles were sold at Suzuki ATV dealers nationwide from July 2007 through February 2011. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml11/11727.html

Kia recalls 70,000 Optimas for transmission defect. Kia Motors is recalling more than 70,000 Optima midsize sedans to fix transmission problems that can cause the cars to roll even while they are in park, Associated Press reported March 11. The cars are from the 2006 through 2008 model years and were built from September 29, 2005 to June 13, 2007. In documents filed with the National Highway Traffic Safety Administration, Kia said that on some of the cars, a transmission shifter cable was installed incorrectly and can become detached from the shifter. If the cable comes off, the car would stay in the last gear used even if the driver puts the transmission in park, the documents said. "If the driver leaves the vehicle without engaging the parking brake, there is a possibility that the vehicle can roll, creating the risk of a crash," Kia said. No injuries have been reported, but Kia concluded that under "extraordinary circumstances" the cars could roll inadvertently. Kia plans to start the recall in

March and will notify owners by mail. Source: http://www.sfgate.com/cgi-bin/article.cgi?f=/n/a/2011/03/11/state/n051947S27.DTL

Global Industrial recalls workbench components due to electrical shock hazard. Global Equipment Company, of Port Washington, New York, doing business as Global Industrial, issued a recall March 9 for about 5,000 Global Workbench power risers, power aprons, and power shelves. Misrouted wiring in the electrical outlets on the workbench risers, aprons, and shelves, and reverse polarity in some workbench power cords pose an electric shock hazard. The manufacturer has received eight reports of misrouted wires. Global Industrial sold the workbench components through its catalogs and on the Internet, from January 9, 2009 to December 24, 2010. Source: http://www.cpsc.gov/cpscpub/prerel/prhtml11/11724.html

Honda, Toyota and Chrysler issue recalls. Honda recalled more than 35,000 Civic hybrids in the United States March 7 to fix a problem with the electrical system that could cause the headlights to turn off or the engine to stall. The company said the voltage converter that relays power from the motor assist system to the vehicle's electrical components could fail. Separately, Toyota recalled about 22,000 SUVs and trucks to address faulty tire pressure monitoring systems. Toyota said the systems do not illuminate on the dashboard at the minimum activation pressure and must be recalibrated. Chrysler recalled about 20,000 Jeep Wranglers over potential loose fasteners to the front and rear axles. The issue could cause poor steering and handling or cause the driver to lose control of the vehicle. Source: http://www.npr.org/templates/story/story.php?storyId=134335459

DEFENSE/ INDUSTRY BASE SECTOR

Counterfeit electronic parts ending up in DoD weapons systems. Faulty counterfeit electronic parts are ending up in the Defense Department's (DOD) weapons systems, and the problem poses a critical risk to national security, according to the U.S. Senate Armed Services Committee. The chairman and ranking member of the committee called the presence of counterfeit electronic parts in the DOD's supply chain a "growing problem" March 9, and announced an investigation into just how they are ending up there. Over the course of its investigation, the committee plans to determine the source and extent of the problem and identify possible solutions. A report by the Department of Commerce in January 2010 found that 39 percent of electronics companies contracted by the Defense Department encountered counterfeit electronics from subcontractors, more than doubling from 2005 to 2008. The semiconductor industry also has expressed concerns that counterfeit chips mislabeled as military-grade can lead to fatal malfunctions in military and aerospace parts. Source: http://tpmdc.talkingpointsmemo.com/2011/03/counterfeit-electronic-parts-ending-up-in-dod-weapons-systems.php

(New Jersey) **Defense contractor charged with stealing secrets on laptop.** A former engineer with U.S. military contractor L-3 Communications is facing as much as 20 years in prison on charges he illegally exported military data to China, IDG News Service reported March 8. He was charged March 4 in United States District Court for the District of New Jersey, but the complaint was not unsealed until March 8, the date the suspect was set to appear in federal court in Chicago. The man was stopped by U.S. Customs and Border Protection officers November 29, 2010, after flying back from a speaking engagement at a highly technical nanotechnology conference hosted by local universities and Chinese government officials. Border agents became suspicious when the agents found a

conference lanyard in his luggage during a secondary inspection at New Jersey's Newark Liberty International Airport. The suspect had said he had been in China to visit family. "Customs officers found a folder containing multiple pages of technical language, pictures of military weapons systems, and documents written in Chinese," wrote an FBI special agent in an affidavit. Border guards also found a laptop. After obtaining a search warrant, federal investigators then discovered hundreds of company documents on the man's computer, including several that contained technical data on guidance and control systems governed by U.S. arms export control laws. Source: http://www.pcworld.com/businesscenter/article/221676/defense_contractor_charged_with_stealing_secrets_on_laptop.html

Man sentenced for defrauding U.S. Navy. Bristol Alloys Inc., and its president who cut corners when manufacturing submarine parts, must repay the U.S. Navy $1.3 million. Besides the money in restitution for the Fairless Hills, Pennsylvania company, a U.S. district court judge March 4 ordered the company president to serve 41 months in federal prison. Bristol and its president pleaded guilty in October 2010 to selling substandard metal to customers. As a subcontractor, Bristol fraudulently supplied a Navy contractor with metal that did not conform to required military specifications and provided counterfeit certifications that purportedly showed that the metal had been heat-treated according to contract requirements. The U.S. prosecutors contended the defendants knew that no such heat treatment had occurred. The metal supplied was used in building Virginia Class submarines and other Navy ships and submarines. Source: http://www.phillyburbs.com/news/local/courier_times_news/article_aafec0bd-0bdc-5fdb-9bb1-11d525f7bc8a.html

China 'hacked' into secret S. Korea military files. Chinese computer hackers in June 2010 gained access to secret South Korean military files on a planned spy plane purchase from the United States, Agence France-Presse reported March 6. The hackers accessed information in defense ministry computers on the plan to buy unmanned Global Hawk aircraft. Information about the breach was revealed by an opposition Democratic Party lawmaker and a member of the parliament's defense committee. Source: http://www.google.com/hostednews/afp/article/ALeqM5hoPjSaKhzX6th7fTgDWFIvH4ePeg?docId=CNG.7131e2b502649c227658543dce51e738.261

Emergency Services

(Pennsylvania) **Suspicious package found, Township buildings evacuated.** A suspicious package was found March 8 near the side of the Marple Police station in Broomall, Pennsylvania, about 7 p.m., prompting the evacuation of the police and municipal buildings and library. According to a Marple police lieutenant, the suspicious package was contained in an approximate 8-inch by 6-inch box. People were safely evacuated out of the buildings at approximately 7:15 p.m., the lieutenant said. "We were just being overly cautious," he said. He said there have been occasions when people have dropped off old war relics to the police department, but the contents of this package are still under investigation. The Delaware County bomb squad also responded. Source: http://marplenewtown.patch.com/articles/suspicious-package-found-township-buildings-evacuated

Product warning and recall notice: Winchester Ranger law enforcement 223 Remington 64 grain power-point. Olin Corporation, through its Winchester Division, is recalling 6 lots of its RANGER 223 Remington 64 Grain Power-Point (PP) centerfire rifle ammunition (Symbol Number RA223R2). Lot Numbers (last four characters): DK01, DK11, DK21, DK31, DK41, and DK51. Through extensive evaluation Winchester has determined the above lots of RANGER Law Enforcement ammunition may contain incorrect propellant. Incorrect propellant in this ammunition may cause firearm damage, rendering the firearm inoperable, and subject the shooter or bystanders to a risk of serious personal injury when fired. Source: http://www.winchester.com/library/news/Pages/News-ProductWarningandRecall.aspx

(New York) **Radio problems from 9/11 not fixed, could strike again.** The communications failures that led to the deaths of hundreds of first responders on 9/11 still have not been fixed, despite tens of millions of dollars spent on elaborate radio systems in lower Manhattan, the New York Post has learned. The Port Authority of New York and New Jersey (PA) February 24 approved $130 million for the design and construction of a massive communications system at the 16-acre World Trade Center site in Manhattan, New York, which the bi-state agency owns. The PA is planning to hard-wire the new buildings at the site and build in transmitters, antennas, and broadcast equipment that would allow emergency workers to communicate even if all power fails and the buildings again come under attack. The problem is the PA is not following recommendations to install a whole new system, but is instead expanding its antiquated radio infrastructure — which is being discontinued by the manufacturer and is not compatible with the emergency communications setup of the New York Police Department (NYPD) and the Fire Department City of New York (FDNY), the agency confirmed. Because of that, sources told the Post, NYPD refused to sign off on the PA's plans and then broke off talks altogether before the agency's board voted unanimously on the spending. Source: http://www.nypost.com/p/news/local/manhattan/radio_shock_waves_4ktnHOr6DUx4eqSYIXTwPO

ENERGY

TransCanada agrees to extra safety steps for proposed pipeline expansion. TransCanada Corporation will voluntarily add extra safety features to a proposed oil sands pipeline expansion that is causing concern among environmentalists and U.S. officials, a company executive said. The pipeline expansion, called the Keystone XL project, would dramatically increase the amount of Canadian crude flowing into the United States and is pending federal approval. The TransCanada executive vice president of operations and major projects said the company agreed to 57 safety measures beyond what is required by law in a deal with the United States. Source: http://online.wsj.com/article/BT-CO-20110310-717078.html

NERC sets up cyber task force to protect power grid. The North American Electric Reliability Corporation (NERC) is setting up a cyber-attack task force to evaluate and help protect the U.S. power grid in the event of a Web assault, according to a release from the electric reliability organization. The 40-volunteer strong task force will identify opportunities to boost existing protection, resilience, and recovery capabilities associated with power system practices, plans, and procedures, as well as the tools and systems operators rely upon to manage the reliable operation of the bulk power system. "Operators are trained to spot anomalies and take the appropriate actions in real time," said the director of IT risk management at Dominion, who also chairs the task force. "The Cyber Attack Task

Force will build on that existing knowledge with recommendations that make it easier to detect and respond to indicators of an organized attack." Last year, NERC and the Energy Department released the report "High-Impact, Low-Frequency Event Risk to the North American Bulk Power System," which found the best approach to handling risks would be through an organized combination of industry-led task forces and NERC staff initiatives. Source: http://www.thenewnewinternet.com/2011/03/04/nerc-sets-up-cyber-task-force-to-protect-power-grid/

(Alaska) **137 oil wells out of compliance.** A report presented to Alaska lawmakers the week of February 28 claims 137 northern Alaska oil wells are out of compliance with state regulations. The wells are relatively old with most having been drilled between 1944 and 1981. According to the Alaskan Oil and Gas Commission, most of the wells are abandoned, and only 10 were properly sealed. Two of those are now under lakes, and a landslide has buried another. Despite the fact the wells appear to violate state and federal rules, the report claimed there is little the state can do to force a cleanup. The paper said the Federal Bureau of Land Management should pay to properly shutter and clean up the old well sites. Source: http://www.ktva.com/home/top-stories/137-Oil-Wells-Out-of-Compliance-117475439.html

Food and Agriculture

(New York) **NY meat maker recalls bologna products.** The U.S. Department of Agriculture's Food Safety and Inspection Service (FSIS) said March 9 Zweigle's Inc. of Rochester, New York, recalled about 3,000 pounds of bologna products that may be contaminated with bacteria. The company recalled cases containing 2, 10-pound packages of "Price Chopper German Brand Bologna Made With Pork & Chicken." The maker of hot dogs, sausages and deli products said the bologna products were packaged January 7, and each package has the establishment number "EST. 5333" within the USDA mark of inspection. A smokehouse malfunction created the potential production of staphylococcus aureus enterotoxin, which can cause nausea, vomiting, diarrhea, and abdominal cramping. Source: http://online.wsj.com/article/APa88cd31a5a58467f90b280fe87d170b5.html

Ground beef products recalled due to possible E. coli. Creekstone Farms Premium Beef, an Arkansas City, Kansas, establishment, recalled approximately 14,158 pounds of ground beef products that may be contaminated with E. coli O157:H7, the U.S. Department of Agriculture's (USDA) Food Safety and Inspection Service (FSIS) announced March 9. According to the USDA Web site, the products were distributed to firms in North Carolina. Each case label bears the establishment number "EST. 27" inside the USDA mark of inspection. These products were produced February 22 and were shipped to firms in Arizona, California, Georgia, Indiana, Iowa, Missouri, North Carolina, Ohio, Pennsylvania, and Washington for further processing and/or distribution. The products may have been repackaged into consumer-size packages and sold under different retail brand names. The problem was discovered through third-party lab results. Source: http://www.citizen-times.com/article/20110309/NEWS/303090062/Ground-beef-products-recalled-due-possible-E-coli?odyssey=mod|newswell|text|Frontpage|s

USDA audit says E. coli testing in ground beef is flawed. The U.S. Department of Agriculture (USDA) has found its process for testing for E. coli in ground beef is flawed and may be missing bacteria

during tests. These findings come from an audit released March 7 by the agency's Inspector General (IG). It warns the current sampling method "is not designed to yield the statistical precision that is reasonable for food safety or to verify that plant controls or interventions are working as intended." The audit makes four recommendations for improving inspections of the nearly 4 billion pounds of ground beef produced annually in the United States. These recommendations include developing a redesigned sampling program to provide "higher confidence" in the testing regime. The audit was done at the request of a U.S. Representative from Connecticut. The IG warned that, in situations where E. coli is present in 1 percent of the inspected bin, the current screening method would miss it more than half the time. Or, as the report puts it, "if the contamination level is very low, FSIS (Food Safety and Inspection Service) is more likely to miss contamination than to detect it." Source: http://www.publicintegrity.org/blog/entry/3000/

Unilever announces recall of Skippy Reduced Fat Peanut Butter Spread due to possible health risk. Unilever United States, Inc. announced March 4 a limited recall of Skippy Reduced Fat Creamy Peanut Butter Spread and Skippy Reduced Fat Super Chunk Peanut Butter Spread, because it may be contaminated with Salmonella. The recall is being conducted in cooperation with the U.S. Food and Drug Administration (FDA). No other Skippy products are affected by this recall. The product was distributed to retail outlets in Arkansas, Connecticut, Delaware, Illinois, Iowa, Maine, Minnesota, Missouri, Nebraska, New Hampshire, New Jersey, New York, North Dakota, Pennsylvania, Virginia, and Wisconsin. Source: http://www.fda.gov/Safety/Recalls/ucm245897.htm

(Oregon) **E. coli contaminated hazelnuts likely from Oregon.** An E. coli outbreak that has caused at least 7 illnesses in Michigan (1), Minnesota (3), and Wisconsin (3) involves hazelnuts likely grown and harvested in Oregon. The three Minnesota infections involved men over age 50 from Hennepin, Stearns, and Redwood counties. Two were hospitalized; all three have recovered. Hazelnuts grow on trees, but they are harvested after they fall to the ground, where the contamination likely occurred, according to an official at the Minnesota Department of Agriculture's dairy and food inspection division. "The fact that they do spend some time on the ground increases the risk of environmental contamination," he said. The investigation is now focusing on farms in Oregon that produce the majority of U.S. hazelnuts. Source: http://www.foodpoisonjournal.com/foodborne-illness-outbreaks/e-coli-contaminated-hazelnuts-likely-from-oregon/

Government Sector (including Schools and Universities)

(Alaska) **Five charged in alleged plot to kidnap or kill troopers, judge.** Five people in the Fairbanks, Alaska, area were arrested March 10 by state and federal law enforcement on charges connected with a plot to kidnap or kill state troopers and a Fairbanks judge, according to the Alaska State Troopers. The Fairbanks police chief said the operation involved multiple police actions related to Fairbanks-area members of the "sovereign citizen" movement. The movement is characterized by a rejection of U.S. laws and taxes. In general, participants believe federal, state and local statutes and laws do not apply to them. The suspects are accused of conspiring to commit murder, kidnapping, and arson, as well as weapons misconduct, hindering prosecution and tampering with evidence, a trooper spokeswoman said in a written statement March 10. An investigation "revealed extensive plans to kidnap or kill Alaska state troopers and a Fairbanks Judge," the statement said. The plans

included "extensive surveillance" on the homes of two Fairbanks troopers, the statement said. "Investigation also revealed that extensive surveillance on troopers in the Fairbanks area had occurred, specifically on the locations of the homes for two Alaska state troopers," the statement said. "Furthermore, [the suspects] had acquired a large cache of weapons in order to carry out attacks against their targeted victims. Some of the weapons known to be in the cache are prohibited by state or federal law." Along with troopers and Fairbanks police, the FBI, and U.S. Marshals Service carried out the arrests. Source: http://www.adn.com/2011/03/10/1748613/man-who-threatened-judge.html

U.S. charges 10 in Ciudad Juarez killings. U.S. authorities said March 9 that they have charged 10 alleged Mexican gang members with murdering two Americans and a Mexican man who had ties to the U.S. consulate in Ciudad Juarez, Mexico. A U.S. Consulate employee and her American husband were gunned down in broad daylight March 13, 2010 as they left an event sponsored by the consulate, which is located just across the border from El Paso, Texas. The suspects, part of the Barrio Azteca gang, were also accused of murdering a Mexican man married to another consulate employee, around the same time in another part of the city after they left the same event. Seven of the 10 defendants are in custody in Mexico, and the United States is working with Mexican authorities to extradite them for prosecution, the Justice Department said. Source: http://www.washingtonpost.com/wp-dyn/content/article/2011/03/09/AR2011030905231.html

(Virginia) **Pentagon takes Anonymous threats seriously.** A new operation launched by members of the Anonymous collective has captured the attention of Pentagon officials who asked law enforcement agencies to investigate the group's actions. According to a Forbes report, Anonymous hacktivists threatened to harass the Department of Defense press secretary and chief warrant officer in retaliation to how a Private First Class (PFC) was being treated at the Quantico Brig in Virginia. Anonymous members launched an offense called Operation Bradical and warned they will "ruin" the lives of their targets if their demands are not met. The PFC "must be given sheets, blankets, any religious texts he desires, adequate reading material, clothes, and a ball," Anonymous said. "One week. Otherwise, we continue to dox and ruin those responsible for keeping him naked, without bedding, without any of the basic amenities that were provided even to captured Nazis in WWII," the group said. Source: http://news.softpedia.com/news/Pentagon-Takes-Anonymous-Threats-Seriously-188464.shtml

CIA website disruption may have been work of a prankster. Federal officials as March 7 were still investigating the cause of a cyber incident March 3 that knocked offline the public Web site of the CIA and its unclassified e-mail system. Some cyber experts said the disruption may have been caused by a denial of service attack perpetrated by pranksters to show off their skills, rather than a terrorist act committed by a foreign government. Contrary to previous news reports, the interference was isolated to CIA networks. The U.S. Computer Emergency Response Team (US-CERT) received no reports from agencies other than the CIA experiencing technical problems with their unclassified Web sites or e-mail systems, Homeland Security Department officials said March 7. The CIA site, which the spy agency recently retooled to attract more visitors, was back online by 11 a.m. March 4, and employee e-mail is also now working, CIA officials said March 7. Source: http://www.nextgov.com/nextgov/ng_20110307_1120.php

INFORMATION TECHNOLOGY AND TELECOMMUNICATIONS

'Most recent earthquake in Japan' searches lead to FAKEAV. According to Trend Micro March 11, blackhat SEO attacks began appearing almost immediately after an 8.9 magnitude earthquake hit Japan and then was followed by a tsunami, causing massive damage. The company began to monitor immediately for any active attacks as soon as the news broke out. Results found Web pages inserted with key words related to the earthquake. One of the active sites used the keyword "most recent earthquake in Japan" and led to FAKEAV variants currently detected as Mal_FakeAV-25. Users were advised to get the latest news from trusted media outlets to prevent being victimized by this blackhat SEO. Source: http://blog.trendmicro.com/most-recent-earthquake-in-japan-searches-lead-to-fakea/

Zeus toolkit with 'ghost' panel for better evasion. The last version of the Zeus builder before its author gave up its source code to the author of the SpyEye toolkit is 2.0.8.9, and it is still being offered on the online black market by resellers. This last version has new and improved features when compared with the previous one, such as support for almost all Windows versions, an injection module for Firefox, and multi-user session session infection. According to Trend Micro researchers, the control panel has remained practically the same. Named "Ghost" panel by the authors, it supposedly has two features that allow it to remain hidden from analysis with automated tools and researchers that search for it in the usual places. One is by using unusual file and folder names, and the other is to block IP addresses of malware-monitoring sites such as ZeuS Tracker when they try to access the Web panel by using a configurable script located in the .htaccess file. The panel presents other advantages such as optimizing PHP scripts for smaller file sizes (to make their upload to hosting sites easier), filtering that only allows the storage of financial information, and an easy and automatic update of the configuration file. Source: http://www.net-security.org/malware_news.php?id=1664

Apple security update leaves iPhone 3G users unprotected. Apple is leaving some of its older mobile devices unprotected with its latest patch batch. An iOS 4.3 update, which includes a number of critical security fixes, is incompatible with the widely used iPhone 3G, and older versions of the iPod Touch. The latest version of Apple's mobile software can only be applied on the iPhone 3GSs and later models; the iPod Touch 3rd generation and later models; as well as all versions of the iPad. Security firm Sophos warned the omission of the fixes leaves users of older iPhone and iPod Touches at heightened risk of drive-by download attacks from harmful Web sites. Source: http://www.theregister.co.uk/2011/03/10/apple_update_omits_iphone3g/

Symantec finds fake Google Android update. Google's latest update for its Android mobile OS appears to already have been subverted by hackers, according to the security vendor Symantec. Symantec found an application called the "Android Market Security Tool" that is a repackaged version of the legitimate update by the same name that removed the DroidDream malware from infected devices. The fake security tool sends SMSes to a command-and-control server, wrote a Symantec representative. The company is still analyzing the code, which it found on a third-party application market targeted at Chinese users. "What is shocking is that the threat's code seems to be based on a project hosted on Google Code and licensed under the Apache License," the Symantec representative wrote. Source: http://www.computerworld.com/s/article/9214023/Symantec_finds_fake_Google_Android_update

Microsoft detects spikes in SWF malware attacks using embedded JavaScript. Microsoft has seen spikes in the number of attacks using SWF malware that embed malicious JavaScript and warn this technique might become more prevalent. SWF-based malware is not new. It is commonly used to exploit vulnerabilities in Adobe Flash Player in order to install further threats on computers. The new trojan identified by Microsoft and dubbed Trojan:SWF/Jaswi.A targets CVE-2010-0806, an arbitrary code execution vulnerability in Internet Explorer 6 and 7. However, what sets it apart is the way the JavaScript-based exploit is launched. Most SWF malware use the getURL function to redirect users to malicious sites, but Jaswi.A uses a function called ExternalInterface.call() to initiate the injection. If successful, the attack downloads a file called uusee(dot)exe, which is a Chinese password stealer known as PWS:Win32/Lolyda(dot)AU. Source: http://news.softpedia.com/news/Microsoft-Sees-Spikes-in-SWF-Malware-with-Embedded-JavaScript-188253.shtml

USB driver bug exposed as 'Linux plug&pwn'. A researcher from MRW InfoSecurity has reported a bug in the Caiaq USB driver that could be used to gain control of a Linux system via a USB device. The bug is caused by the device name being copied into a memory area with a size of 80 bytes using strcpy() without its length being tested. A crafted device with a long device name could thus write beyond the limits of this buffer, allowing it to inject and execute code. Because the driver is included, and automatically loaded, in most Linux distributions, to execute code in kernel mode an attacker would merely have to connect such a device to a Linux system's USB port. MRW said it has assembled a suitable USB device for this purpose, boasting in a Tweet of a "Linux plug&pwn." Source: http://www.h-online.com/security/news/item/USB-driver-bug-exposed-as-Linux-plug-pwn-1203617.html

DHS needs to change rules to recruit hackers into U.S. security agencies. Hackers and other computer experts willing to collaborate with DHS to bolster the nation's cyber-defense are unable to do so because of red tape, according to the former head of the department. Two former secretaries of Homeland Security joined the head of DHS to discuss the evolution of threats facing the United States, including the challenges of securing cyber-space. They expressed their views during a March 2 roundtable discussion at Georgetown University, which was webcast by the Aspen Institute. There are a number of possible scary scenarios, including a sophisticated hacker from another country breaking into the power grid or other critical infrastructure and shutting things down, a Trojan that wipes out information on government computers, or even steals sensitive documents. The Department of Defense and DHS currently work together on cyber-defense. The federal government is short "tens of thousands of cyber experts" and is aggressively hiring, according to NextGov. A former CIA official estimated that about 1,000 security experts in the nation possess the skills to safeguard U.S. cyberspace, but the country needs about 30,000, according to Government Executive. Source: http://www.eweek.com/c/a/Security/DHS-Needs-to-Change-Rules-to-Recruit-Hackers-into-US-Security-Agencies-252689/

National Monuments and Icons

(Washington) **Illegal dumping on Washington State trust lands costs hundreds of thousands of dollars to taxpayers annually.** The Washington State Department of Natural Resources (DNR) announced March 10 a new interactive online map showing locations of more than 200 sites that experienced illegal dumping in 2010 on state trust lands. DNR, along with the department of ecology

and other agencies, spend hundreds of thousands of dollars each year to clean up household trash, junked vehicles, and commercial and hazardous waste dumped illegally on state trust lands. Illegal dumping often occurs near forest roads on the 2.1 million acres of forestland DNR manages to generate revenue for public schools and local services. Hazardous sites, such as discarded industrial solvents or meth labs, can cost thousands of dollars each to clean up. Sending trucks to remote locations to remove abandoned vehicles also is costly. DNR's chief of law enforcement services said the online map is intended to show the extent of illegal dumping. The map shows locations of the 49 abandoned vehicles, 32 commercial and hazardous waste dumps, and 113 household dumping sites DNR's Law Enforcement Service investigated in 2010. Source: http://www.dnr.wa.gov/RecreationEducation/News/Pages/2011_03_10_dumping_nr.aspx

(Missouri) **Vandals target Wilson's Creek National Battlefield.** A maintenance worker at Wilson's Creek National Battlefield in Republic, Missouri, noticed March 7 one of the cannons at Guibor's Battery did not look right. Vandals had stolen a component known as an elevation screw from one of thec guns and cut the cables holding another in place. The worker notified a law enforcement park ranger, who searched the rest of the park for further damage. The ranger found a cannon at Bloody Hill had been cut free from its moorings and moved in front of another, muzzle to muzzle. And at Pulaski Battery, the cannon had been cut loose and rolled down a large hill. The barrel had come free of the carriage, leaving a large scrape along the side. The carriage itself was also significantly damaged in the incident. Source: http://www.kspr.com/news/local/kspr-vandals-target-wilsons-national-battlefield-20110308,0,98764.story

Postal and Shipping

(Alabama) **UNA staffer suspended after suspicious mail incident.** The University of North Alabama in Florence, Alabama, said March 4 it suspended an employee suspected of sending a threatening letter that prompted the evacuation of a campus building. The school said the unidentified staff member was placed on unpaid leave and barred from the school. A university spokesman said the person is prohibited from contacting anyone on the northwest Alabama campus. No charges have been filed, but the case is being turned over to state prosecutors and federal postal inspectors. Authorities evacuated Stevens Hall after a threatening letter containing white powder was delivered March 3. Officials said it was addressed to a faculty member. There is no word yet on what the powder was. Source: http://www.waaytv.com/news/local/story/UNA-Staffer-Suspended-After-Suspicious-Mail/aBFhUjc-40K_WDUm5kLamw.cspx

Public Health

FDA to oversee J&J plants after flood of recalls. U.S. health authorities will take over supervision of three Johnson and Johnson manufacturing plants after the healthcare giant failed to stem a flood of recalls for consumer medicines such as its Tylenol painkiller. The company's McNeil unit has recalled more than 300 million bottles and packages of Tylenol, Motrin, Rolaids, Benadryl, and other products in the past year over faulty manufacturing. The U.S. Food and Drug Administration said the action, called a consent decree, prevents McNeil from making consumer medicines at a large plant in Fort Washington, Pennsylvania, until the agency certifies quality lapses there have been corrected. It also sets a strict timetable to rectify manufacturing problems at McNeil's plants still operating in Lancaster, Pennsylvania and Las Piedras, Puerto Rico. J&J said two company executives were named

as defendants in the consent decree. They are the vice president of quality at J&J's McNeil Consumer Healthcare unit, and the vice president of operations at McNeil. Some of the lapses led to metal particles entering liquid medicines, and also included mislabeling and moldy odors. Source: http://www.reuters.com/article/2011/03/10/johnsonjohnson-idUSN1017286320110310

Under pressure, firm closes line that made tainted wipes. A Wisconsin medical supplier that made millions of recalled alcohol prep products now blamed for serious infections and at least one death is shutting down the line that produces the wipes — at least for now. The Triad Group of Hartland, Wisconsin, plans to "move away" from its health care division, which produced contaminated alcohol pads and lubricating jelly, and focus instead on its private label and contract brands, according to an internal letter obtained by msnbc.com. The letter was prompted in part by a series of msnbc.com reports detailing potentially life-threatening problems with contamination at the plant. Triad officials made the move voluntarily and did not notify the U.S. Food and Drug Administration (FDA) about their plans to halt production of alcohol prep products named in a January 3 recall because of potential contamination, an FDA spokeswoman said. Triad will also stop production of sterile lubricating jelly, which was the focus of a December 27, 2010 recall and has been tied to reports of vaginal infections that required medication for dozens of women. The prep pads and jelly are the two largest product lines in that division, Triad's chief operating officer said. FDA has issued no sanctions, despite government documents that identified ongoing problems with contamination and sterilization at the Triad plant dating back to at least 2009. FDA inspectors detected microbial contamination in wipes and jelly, and problems with validation of Triad's sterilization process, documents show. Source: http://today.msnbc.msn.com/id/42018220/ns/health-infectious_diseases/

CDC develops crisis response toolkit for public health response authorities. The Centers for Disease Control and Prevention's (CDC) National Center for Environmental Health, Division of Environmental Hazards and Health Effect Health Studies Branch has produced the Community Assessment for Public Health Emergency Response (CASPER) Toolkit to address challenges public health and other emergency response officials confront in identifying, preparing for, responding to, and mitigating disasters, such as large-scale outbreaks. CASPER was specifically designed to help epidemiologists and public health authorities in the collection of important health intelligence during a large-scale, potentially mass casualty disaster. CASPER, also referred to as Rapid Need Assessment (RNA), Rapid Epidemiologic Assessment (REA), and Rapid Health Assessment (RHA), "will assist public health practitioners and emergency management officials in determining the health status and basic needs of the affected community," the guidance explained, noting "gathering information about health and basic need data by using valid statistical methods allows public health and emergency managers to prioritize their responses and to rationalize the distribution of resources." "Personnel from any local, regional, state or federal public health department, emergency management officials, academicians or other disaster responders who need to assess household-level public health needs following a disaster may use this toolkit." The main objective of CASPER is to rapidly assess the present and potential health effects and basic needs for a population affected by a disaster. Source: http://www.hstoday.us/briefings/today-s-news-analysis/single-article/cdc-develops-crisis-response-toolkit-for-public-health-response-authorities/3ceaf7dea2c853033ec6aa0e8f963df4.html

TRANSPORTATION

(Georgia; North Carolina) **Augusta flight threatened.** An Augusta, Georgia man could face federal charges after he made a threat against a plane he was waiting to board March 10 at Augusta Regional Airport in Augusta, Georgia, a Richmond County sheriff's sergeant said. The suspect, 22, of Morgan Road, was waiting for his 8:25 p.m. flight to Charlotte, North Carolina, inside the airport terminal when he phoned someone he knew and made the threat, the sergeant said. He would not disclose the exact threat or say who the call was made to, just that it was "terroristic" in nature. Authorities searched the plane after it landed, and the entire airport, but they did not find anything. The suspect was arrested on a charge of terroristic acts and threats. The FBI is assisting in the investigation, the sergeant said. He said the Augusta man indirectly made a threat against the pilot and airline through a text message sent while he waited in the airline terminal. The person the man was texting notified the sheriff's department with concerns. Source: http://chronicle.augusta.com/latest-news/2011-03-10/augusta-flight-threatened?v=1299804167

U.S., EU near air-safety pact. After a delay of almost 2 years, the United States and the European Union (EU) appear ready to cement an air-safety pact that both sides said should improve aviation oversight and save millions of dollars annually by eliminating duplicate efforts. The agreement was reached in 2008 but languished amid opposition in the U.S. Congress. That fight now appears resolved. As a result, the EU gave its final approval of the pact March 7, which could come into force as soon as May 1. Under the deal, U.S. and EU air-safety agencies will recognize each other's inspections and analysis. That should allow the U.S. Federal Aviation Administration and the European Aviation Safety Agency to share data and avoid duplicating efforts, officials said. The coordination also will help harmonize air-safety rules in the world's two biggest aviation markets, reducing costs and confusion for airlines, pilots, and manufacturers. In coming days, the two sides expect to exchange diplomatic notes, officially sealing the pact, the Agreement Between the U.S. and the European Community on Cooperation in the Regulation of Civil Aviation. Source: http://online.wsj.com/article/SB10001424052748703662804576188622512907848.html

Airlines remove oxygen units in fire threat. According to industry sources, U.S. airlines have quietly removed oxygen devices from the bathrooms on 6,000 aircraft, responding to Federal Aviation Administration (FAA) concerns that an unobserved passenger could trigger a fire using such a device, TheStreet.com reported March 4. The FAA issued an airworthiness directive February 10 ordering the removals, with the work to be completed within 21 days after each airline received the directive, the sources said. All work was expected to be completed within a few days. Airlines have been able to accomplish the work during routine maintenance. Additionally, the agency alerted foreign aviation regulatory authorities, and some have ordered carriers in their countries to follow the same policy, sources said. The danger was "you could take the generator and [manipulate] it to create a hazard," said am aviation safety consultant, a former member of the National Transportation Safety Board. "You could have an oxygen-fed fire that would be extremely hot." Source: http://www.thestreet.com/story/11031809/1/airlines-remove-oxygen-devices-in-fire-threat.html?cm_ven=GOOGLEN

Water and Dams

EPA submits for public comment the next round of Safe Drinking Water Act contaminant monitoring. The U.S. Environmental Protection Agency (EPA) has proposed 30 currently unregulated contaminants for monitoring in water systems, and submitted the proposal for public comment. Under the authority of the Safe Drinking Water Act (SDWA), EPA regulates more than 90 contaminants in drinking water. To keep drinking water standards up-to-date with emerging science, SDWA requires EPA to identify up to 30 unregulated contaminants for monitoring every 5 years. This current proposal is the third Unregulated Contaminant Monitoring Regulation and includes requirements to monitor for 2 viruses and 28 chemical contaminants that could be present in drinking water and do not currently have health-based standards. EPA is seeking public comment on the proposed list of 30 contaminants until May 2, 2011. Following the public comment period, EPA will review the input before the list is scheduled to be finalized in 2012, with sampling to be conducted from 2013 to 2015. Sampling will take place at all systems serving more than 10,000 people, and at a representative sampling of systems serving less than 10,000 people. Source: http://yosemite.epa.gov/opa/admpress.nsf/1e5ab1124055f3b28525781f0042ed40/713bc83b19ccad9d85257848006f0aac!OpenDocument

North Dakota Homeland Security Contacts

To report a homeland security incident, please contact your local law enforcement agency or one of these agencies: Fusion Center (24/7): 866-885-8295(IN ND ONLY); Email: ndslic@nd.gov ; Fax: **701-328-8175**
State Radio: 800-472-2121 Bureau of Criminal Investigation: 701-328-5500 Highway Patrol: 701-328-2455
US Attorney's Office Intel Analyst: 701-297-7400 Bismarck FBI: 701-223-4875 Fargo FBI: 701-232-7241

To contribute to this summary or if you have questions or comments, please contact:

Kirk Hagel, ND Division of Homeland Security kihagel@nd.gov, **701-328-8168**